Il futuro della Privacy

Avv. Monica Gobbato

28 Maggio 2010

Firenze

www.monicagobbato.it

www.privacyintasca.it

Privacy in TASCA

Programma di lavoro 2010-2011
del Gruppo di lavoro
istituito ai sensi dell'articolo 29 della direttiva 95/46/CE
15 Febbraio 2010

The Future of Privacy
Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data
1 Dicembre 2009

I - Assicurare la corretta applicazione del quadro giuridico vigente e preparare il futuro

* Interpretare le disposizioni chiave della direttiva 95/46/CE e integrare la disciplina (**responsabile del trattamento/incaricato del trattamento, consenso, trasparenza, notifica, obbligo di Notifica della Violazione**)

- II - Affrontare la globalizzazione

* Sviluppare norme vincolanti per le imprese
* Armonizzione delle discipline nazionali

Partecipare ai lavori sulla standardizzazione (per esempio, ISO)

* Conformarsi alle norme internazionali
•

III – Affrontare le Sfide tecnologiche

Privacy by Design: Integrare i Principi Privacy nelle impostazioni di default dei servizi IT (**Punto 46**. Questo principio dovrebbe essere vincolante per progettisti e produttori, nonché per i titolari del trattamento che devono decidere in merito alla acquisizione e uso delle TIC. Essi dovrebbero essere obbligati ad adottare misure protettive già in fase di pianificazione delle informazioni tecnologiche. I fornitori di tali sistemi o servizi, nonché i Titolari devono dimostrare di aver adottato tutte le misure necessarie per conformarsi a tali requisiti). Punto 48 Esso dovrebbe essere un requisito fondamentale per i prodotti ei servizi forniti a terzi e singoli clienti (ad esempio i router WiFi, social network e motori di ricerca)

Motori di ricerca e diritto all'oblio

Siti di social network

Valutazione dell'impatto delle **applicazioni RFID sulla privacy**

IV - Migliorare l'efficacia del Gruppo di lavoro e quella delle autorità per la protezione dei dati

* **Riflettere sul ruolo del Gruppo di lavoro**
* **Rafforzare l'applicazione delle regole** (sviluppare e migliorare i metodi d'indagine, armonizzare i poteri delle autorità per la protezione dei dati e promuovere la cooperazione internazionale tra dette autorità)

I - Assicurare la corretta applicazione del quadro giuridico vigente e preparare il futuro

Semplificazioni per la Notifica

Punto 84 **Le Comunicazioni delle operazioni di trattamento alle Autorità potrebbero essere semplificate o diminuite.**

Punto 85 La Notifica contribuisce ad aumentare la consapevolezza dei trattamenti dei dati e delle pratiche di protezione dei dati all'interno delle aziende.

Essa offre inoltre una panoramica delle attività di trattamento dei dati. Tuttavia, una migliore governance dei dati può raggiungere gli stessi scopi.

I - Assicurare la corretta applicazione del quadro giuridico vigente e preparare il futuro

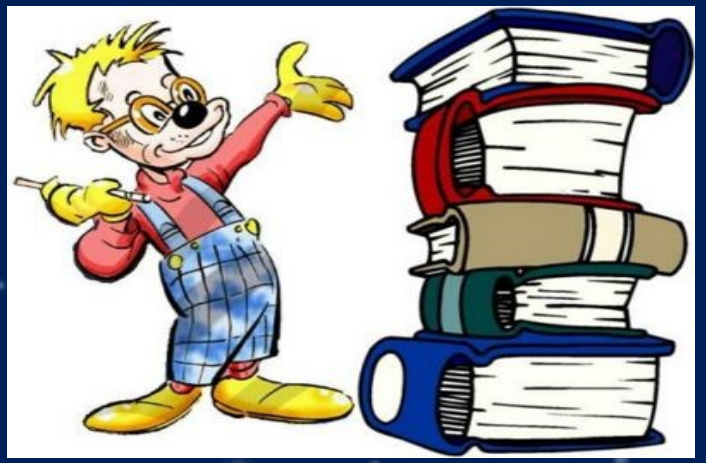
Trasparenza

Punto 63 La trasparenza è requisito fondamentale, in quanto dà alla persona interessata voce in capitolo 'ex ante', prima della trattamento. **Profiling, pubblicità comportamentale, data mining *("estrazione di informazione utile da insiemi di dati***") e sviluppi tecnologici che facilitano l'intercambiabilità dei dati personali rendono ancora più importante conoscere "**chi, su che cosa per quali motivi, da dove e con quali mezzi tecnici si trattano i dati". E 'importante che queste informazioni siano davvero comprensibili.** Tuttavia, il dovere di informare la persona interessata non è sempre adeguatamente messo in pratica. Un nuovo quadro normativo dovrebbe fornire soluzioni alternative, al fine di accrescere la trasparenza.

I - Assicurare la corretta applicazione del quadro giuridico vigente e preparare il futuro

Consenso

Punto 68 L'articolo 7 della direttiva 95/46/CE non è sempre correttamente applicato, in particolare nel contesto di internet, in cui il consenso implicito non conduce sempre a un consenso inequivocabile



I - Assicurare la corretta applicazione del quadro giuridico vigente e preparare il futuro

Obbligo di Notifica della Violazione

Punto 64 Secondo il principio di trasparenza ai singoli interessati dovrebbe essere notificato ogniqualvolta si verifichi una violazione della privacy. Ciò consentirebbe alle persone interessate di controllare gli eventuali danni che tale violazione potrebbe infliggere. (In alcuni casi si potrebbe prevedere l'obbligo di Notifica anche alle Autorità).

I - Assicurare la corretta applicazione del quadro giuridico vigente e preparare il futuro

Misure di sicurezza scalabili

Punto 80 Le misure di sicurezza dovrebbero essere scalabili e prendere in considerazione il tipo di società, la dimensione, il tipo di responsabilità se limitata o illimitata, natura e la quantità dei dati personali trattati, ecc.

I - Assicurare la corretta applicazione del quadro giuridico vigente e preparare il futuro

Migliorare i meccanismi di ricorso della persona interessata

Punto 58 E' necessario che la persona interessata abbia più opzioni per eseguire e far valere i suoi diritti

La possibilità per le procedure di class action dovrebbe essere introdotta dalla direttiva 95/46/CE.

- II - Affrontare la globalizzazione

Punto 29 Stanno diventando indispensabili Standard globali in materia di protezione dei dati

I flussi transfrontalieri di dati a causa della globalizzazione, sono diventati la regola piuttosto che l'eccezione. Occorrono norme a livello mondiale.

- II - Affrontare la globalizzazione

La 'Risoluzione di Madrid',

Proposta comune sulle norme internazionali per la Tutela della Privacy adottata dalla Conferenza Internazionale di Protezione dei dati e della privacy, il 6 novembre 2009.

La proposta prevede un progetto di standard mondiale che riunisce tutti i possibili approcci per la protezione dei dati personali e, l'integrazione della legislazione dei cinque continenti.

Comprende una serie di principi, diritti e obblighi che dovrebbe essere la base per la protezione dei dati in qualsiasi sistema giuridico di tutto il mondo.

- II - Affrontare la globalizzazione

Armonizzazione

PUNTO 70. Attualmente il potere degli interessati è compromesso dalla mancanza di armonizzazione tra le leggi nazionali di attuazione della direttiva 95/46/CE. Parecchi elementi sostanzali (quali le responsabilità e la possibilità di chiedere i danni immateriali) non sono state attuate da tutti gli Stati membri. Poiché la globalizzazione aumenta queste differenze - che indeboliscono la posizione degli interessati – la situazione deve essere sanata.

- II - Affrontare la globalizzazione

Il ruolo dell'interessato su Internet

Sempre più spesso, gli individui caricano i propri dati personali su Internet (social network, servizi di cloud computing, ecc.) La direttiva 95/46/CE non si applica alla persona che carica i dati per scopi 'puramente personali'.

il risultato è un situazione di mancanza di garanzie che deve poter essere affrontata, soprattutto visto il successo di tali servizi.

Principio di Responsabilità

Il Gruppo ritiene opportuno introdurre nel quadro globale **un principio di responsabilità.** In conformità a tale principio, i responsabili del trattamento sarebbero tenuti a effettuare le misure necessarie per garantire che i principi di fondo e gli obblighi della direttiva in vigore siano rispettati.. Tale disposizione permetterebbe di ampliare la necessità di porre in **atto politiche e meccanismi per rendere efficaci i principi di merito e gli obblighi della direttiva in vigore.** Inoltre, il principio di responsabilità richiede responsabili del trattamento per avere interno meccanismi necessari in atto per dimostrare la conformità alle parti interessate esterne, compresi DPA nazionale.

IV - Migliorare l'efficacia del Gruppo di lavoro e quella delle autorità per la protezione dei dati

Compiti del Gruppo di lavoro

Il Gruppo di lavoro è istituito dall'articolo 29 della direttiva 95/46/CE e, a norma dell'articolo 30, paragrafo 1, **ha i seguenti compiti:**

a) **esaminare ogni questione attinente all'applicazione delle norme nazionali** di attuazione della direttiva per **contribuire alla loro applicazione omogenea**;

b) **formulare,** ad uso della Commissione, **un parere sul livello di protezione nella Comunità e nei paesi terzi;**

c) **consigliare la Commissione in merito a ogni progetto di modifica della direttiva,** nonché,

d) **formulare un parere sui codici di condotta** elaborati a livello comunitario.

IV - Migliorare l'efficacia del Gruppo di lavoro e quella delle autorità per la protezione dei dati

Autorita' Nazionali

Al momento, ci sono grandi differenze per quanto riguarda la posizione del DPA nei 27 Stati membri. Ciò è dovuto alle differenze di storia, di giurisprudenza, di cultura e di organizzazione interna degli Stati membri, ma anche perché l'articolo 28 della direttiva 95/46/CE, manca di precisione sotto diversi aspetti.

IV - Migliorare l'efficacia del Gruppo di lavoro e quella delle autorità per la protezione dei dati

Le nuove sfide per la protezione dei dati (globalizzazione e ai cambiamenti tecnologici,) richiedono una vigilanza rigorosa da parte delle DPA. Il nuovo quadro dovrebbe garantire standard uniformi, e il ruolo consultivo delle Autorità nel processo decisionale e legislativo. Grande importanza deve essere data alla gestione dei reclami.

IV - Migliorare l'efficacia del Gruppo di lavoro e quella delle autorità per la protezione dei dati

Indipendenza delle Autorità

Le autorità responsabili della protezione dei dati devono essere pienamente e realmente indipendenti.

Nel nuovo quadro normativo le autorità responsabili della protezione dei dati dovrebbero essere fornite:

IV - Migliorare l'efficacia del Gruppo di lavoro e quella delle autorità per la protezione dei dati

- Totale indipendenza istituzionale (senza essere subordinata a qualsiasi altra autorità governativa).
- Indipendenza funzionale

Le Autorità devono avere un ruolo consultivo anche nei progetti di legge, non solo nei provveimenti amministrativi.

Le Autorità devono avere infrastrutture adeguate per effettuare operazioni senza interruzioni

Le Autorità devono avere risorse adeguate.

IV - Migliorare l’efficacia del Gruppo di lavoro e quella delle autorità per la protezione dei dati

Le autorità devono assumersi responsabilità per l'uso che fanno del loro nuovo potere. Dovranno essere trasparenti e riferire pubblicamente sulle proprie modalità e priorità di azione.

IV - Migliorare l'efficacia del Gruppo di lavoro e quella delle autorità per la protezione dei dati

Cooperazione Internazionale

L'Articolo 29 della direttiva 95/46/CE ha istituito il gruppo per la tutela delle persone fisiche con riguardo al trattamento dei dati personali (WP29) quale organismo istituzionale per la cooperazione tra DPA nazionali. Il WP29 ha un carattere consultivo e agisce in modo indipendente. Suoi compiti sono indicati nell'articolo 30, paragrafo 1 della direttiva e comprendono **contribuire all'applicazione uniforme della direttiva,** esaminando le questioni riguardanti l'applicazione delle misure nazionali, dando pareri sul livello di tutela nella Comunità e nei paesi terzi, nonché **consulenza (anche di propria iniziativa) sulle proposte di legislazione comunitaria** che incidono sulla protezione dei dati.

IV - Migliorare l’efficacia del Gruppo di lavoro e quella delle autorità per la protezione dei dati

Con l'entrata in vigore del trattato di Lisbona, si creeranno nuove prospettive per la legge in materia di protezione dei dati.

Parere 1/2010
sui concetti di
"Titolare del trattamento" e
"Responsabile del trattamento"
adottato il 16 febbraio 2010

I RUOLI DEI DUE SOGGETTI NON ANCORA BEN DEFINITI IL GRUPPO INTERVIENE

La liceità del trattamento dei dati da parte del Responsabile è determinata dal **mandato** ricevuto dal Titolare. **Se va al di là del proprio mandato** e se acquisisce un ruolo rilevante nella determinazione delle finalità o degli aspetti fondamentali dei mezzi del trattamento **il Responsabile diventa (con)Titolare.**
La delega può tuttavia comportare un certo grado di discrezionalità sul modo in cui servire al meglio gli interessi del Titolare del trattamento, consentendo al Responsabile di scegliere gli strumenti tecnici ed organizzativi più adatti.

Rapporto e Linee-Guida in materia di privacy nei servizi di social network (*)
"Memorandum di Roma"
Adottato in occasione del 43mo incontro, 3-4 marzo 2008, Roma

30ma Conferenza internazionale delle Autorità di protezione dei dati
Stasburgo, 15 - 17 ottobre 2008
Risoluzione sulla tutela della privacy nei servizi di social network

Parere 5/2009 sui social network on-line adottato il 12 giugno 2009

Un ricercatore tedesco ha di recente individuato, in un campione di servizi di social network circa 120 attributi personali all'interno dei profili utente, quali ad esempio età, indirizzo, film preferiti, libri preferiti, preferenze musicali, ecc. oltre a opinioni politiche e, addirittura, orientamenti sessuali.

"Memorandum di Roma"
3-4 marzo 2008, Roma

- **La maggioranza dei dati personali pubblicati attraverso servizi di questo tipo sono resi pubblici su iniziativa degli stessi utenti e in base al loro consenso.**

- Le norme "tradizionali" in materia di privacy dettano regole che tutelano i cittadini dal trattamento sleale o sproporzionato dei loro dati personali da parte dei soggetti pubblici e delle imprese. **Vi sono pochissime norme che disciplinino la pubblicazione di dati personali su iniziativa dei singoli.**

Nuova Generazione di Utenti ***Si tratta della prima generazione cresciuta insieme ad Internet. Questi "indigeni digitali" hanno sviluppato approcci del tutto peculiari rispetto al concetto di privato ovvero pubblico. Inoltre, essendo in buona parte adolescenti, sono probabilmente più disposti a mettere a rischio la propria privacy rispetto agli "immigrati digitali"con qualche anno di più.***

I rischi sinora individuati in rapporto all'utilizzo di servizi di social network sono i seguenti:

1) Niente oblio su Internet. Il concetto di oblio non esiste su Internet. I dati, una volta pubblicati, possono rimanerci letteralmente per sempre – **anche se la persona interessata li ha cancellati dal sito "originario", possono esisterne copie presso soggetti terzi.**

- ***2) L'idea ingannevole di "comunità".*** Molti fornitori affermano di trasferire le strutture comunicative dal mondo "reale" al cyberspazio. Un'affermazione frequente è che non ci sarebbero problemi, per esempio, a pubblicare dati (personali) su queste piattaforme, perché è come se si condividessero informazioni con un gruppo di amici nel mondo reale.

- ***3) "Gratis" non sempre significa "a costo zero"***. In realtà, molti dei servizi di social network fanno "pagare" gli utenti attraverso il riutilizzo dei dati contenuti nei profili personali da parte dei fornitori di servizio, ad esempio per attività (mirate) di marketing.

- ***4) La raccolta di dati di traffico da parte dei fornitori di servizi di s. n.*** i quali **hanno gli strumenti tecnici per registrare ogni singolo passo dell'utente sul loro sito** .

- ***5) Utilizzo improprio dei profili utente da parte di soggetti terzi.*** **A seconda della configurazione (di default) disponibile, le informazioni contenute nel profilo (comprese immagini, che possono ritrarre sia il singolo interessato, sia altri soggetti) diventano accessibili all'intera comunità degli utenti.**

6) Rivelare più informazioni personali di quanto si creda.

Linee-guida

Alla luce delle considerazioni svolte il Gruppo di lavoro formula le seguenti raccomandazioni destinate rispettivamente **ai soggetti deputati a disciplinare i servizi di social network, ai fornitori di tali servizi ed agli utenti:**

Prevedere la possibilità di ricorrere a pseudonimi –

Fare in modo che i fornitori di questi servizi adottino un approccio trasparente nell'indicare le informazioni necessarie per accedere al servizio-base, in modo che gli utenti siano in grado di scegliere a ragion veduta se aderire o meno al singolo servizio, e di opporsi ad eventuali utilizzi secondari, in particolare per quanto riguarda forme (mirate) di marketing. ***Introdurre l'obbligo di notifica di eventuali violazioni dei dati relativamente ai servizi di social network*.** L'unico modo per consentire agli utenti di fare fronte, in particolare, al rischio crescente di furti di identità consiste nel notificare loro ogni violazione della sicurezza dei dati. ***Ripensare l'attuale assetto normativo con riguardo alla titolarità* dei dati personali** (in particolare relativi a soggetti terzi) pubblicati sui siti di social network, al fine eventualmente di attribuire ai fornitori di servizi di social network maggiori responsabilità rispetto alle informazioni di natura personale presenti su tali siti.

***Potenziare l'integrazione delle tematiche connesse alla privacy nel sistema educativo*.** Rivelare informazioni personali online è sempre più un fatto normale, soprattutto fra i giovani; pertanto, è necessario che i programmi didattici affrontino tematiche connesse alla privacy ed agli strumenti di autotutela disponibili. **L'informativa resa all'utente deve prendere in considerazione anche i dati relativi a soggetti terzi.** I fornitori dei servizi di social network, **dovrebbero indicare anche ciò che agli utenti è permesso o non permesso fare con i dati relativi a terzi eventualmente contenuti nei rispettivi profili** –

Parere 1/2008 sugli aspetti della protezione dei dati connessi ai motori di ricerca adottato il 4 aprile 2008

Parere 4/2007 sulla Definizione di Dati Personali 20 giugno 2007

DIRETTIVA 2009/136/CE DEL PARLAMENTO EUROPEO E DEL CONSIGLIO
del 25 novembre 2009
recante modifica della direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica, della direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche e del regolamento (CE) n. 2006/2004 sulla cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa a tutela dei consumatori

61 Una violazione di dati personali può, se non è trattata in modo adeguato e tempestivo, provocare un grave danno economico e sociale, tra cui l'usurpazione d'identità, all'abbonato o alla persona interessata. Pertanto, il fornitore di servizi di comunicazione elettronica accessibili al pubblico, non appena viene a conoscenza del fatto che si è verificata tale violazione, dovrebbe notificarla all'autorità nazionale competente. È opportuno che gli abbonati o le persone i cui dati e la cui vita privata potrebbero essere pregiudicati da tali violazioni siano informati tempestivamente per permettere loro di adottare le precauzioni necessarie. Si considera che una violazione pregiudica i dati o la vita privata di un abbonato o di una persona quando implica, ad esempio, il furto o l'usurpazione d'identità, il danno fisico, l'umiliazione grave o il danno alla reputazione in relazione con la fornitura di servizi di comunicazione accessibili al pubblico nella Comunità. È opportuno che la comunicazione includa informazioni sulle misure adottate dal fornitore per affrontare la violazione così come raccomandazioni per gli abbonati o le persone coinvolti.

Grazie…

Avv. Monica Gobbato

www.monicagobbato.it

gobbatomonica@tiscali.it

www.privacyintasca.it